OIPE JC155
JUL 1 8 2005
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of :

Appl. No.	:	09/435,899	Confirmation No. 5856
Applicant	:	P. J. Seger	
Filed	:	11/08/1999	
TC/A.U.	:	2175	
Examiner	:	J. F. Betit	
Docket No.	:	TU999050US1	

Title: WIRELESS SECURITY ACCESS MANAGEMENT FOR A PORTABLE DATA STORAGE CARTRIDGE

FOURTH DECLARATION UNDER 37 C.F.R. Section 1.132

I, Paul M. Greco, declare and say:

That I am a citizen of the United States of America and I reside at 2791 W. Woodview Crest Drive, Tucson, AZ 85742, USA.

That I am a Senior Programmer at IBM Systems Group, in the field of tape drive microcode development, since April 1996.

That I was previously a Senior Design Engineer at Environmental Systems Products, Inc., in the field of code and systems architecture and development, from August 1990 to April 1996.

That I attended college from 1987 to 1988 at the University of Arizona, located in Tucson, AZ.

That I am knowledgeable in the technology and science of Computer Science and Computer Engineering.

1) Present U. S. Patent Application Serial No. 09/435,899

That I have reviewed the present U. S. Patent Application Serial No. 09/435,899, and find that it describes "a portable security system *** which resides in a portable data storage cartridge for managing access to the portable data storage cartridge". (Page 3, lines 13-16).

a) Portable security of access is conducted by combining a user authentication message from the user with a unique user identifier which is in a user table of the portable data storage cartridge.

In the words of the claims, e.g. Claim 1, "A portable security system for managing access to a portable data storage cartridge, said data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in said data storage drive, said portable security system comprising:

"a wireless interface mounted in said portable data storage cartridge for receiving power and data from, and sending data to, said data storage drive when mounted in said data storage drive; and

"a computer processor mounted in said portable data storage cartridge and coupled to said wireless interface; said computer processor powered by said wireless interface and receiving and transmitting data to said data storage drive via said wireless interface; said computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user; said computer processor receiving said user authentication messages from said data storage drive via said wireless interface, combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity, and transmitting said user authorization or denial to said data storage drive via said wireless interface."

2) International Publication No. WO 87/07062, Anderl et al.

That I have reviewed International Publication No. WO 87/07062, Anderl et al., and find that it relates to a "high security portable data carrier system ***" (Page 2, lines 7-8), with "an executive operating system that is accessed from the station via a set of *** command primitives" which "manipulate the card file system in accord with rules required by card security" (Page 2, lines 17-20).

I-III) The discussion of Anderl et al. of my Second Declaration Under 37 C.F.R. Section 1.132 is incorporated herein.

a) "Security for the card is provided by requiring a separate password for gaining access to each of designated levels of interaction between the card and the associated station." (Anderl et al. Page 2, lines 27-29) (emphasis added). "This password is checked internally by the card algorithmically against the appropriate password at the same login level in the card header." (Page 11, lines 16-18) (emphasis added). Any authentication (not directly described) appears to be of the "card" or "file" and not the "user", see Page 7, lines 9-19.

Thus, Anderl et al. access security is provided by an entirely different mechanism than the present '899 Application's claims "combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm, to authorize or deny said user activity."

Specifically, Anderl et al. have no "user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media", and no ability to combine "said user authentication message with at least part of said user identifier from said user table" of the claims of the present '899 Application.

b) Anderl et al. appears to fail to provide a truly portable security access system.

Rather, Anderl et al. discuss establishment of access at issuance by the issuer at a particular station. "The high security header 35 contains information such as *** the passwords for each login level ***. Direct access to the header section is available only to the two top security levels." (Page 9, lines 4-9). "The fourth level of security is that retained by the MASTER ISSUER. It is at this level that the card is formatted and from which it is issued. *** Each account in this example is handled by a separate file on the card and only persons or programs with the proper credentials for a particular file may access that file at an appropriate application station." (Page 8, lines 6-15) (Emphasis added).

Thus, Anderl et al. access is established at issuance of the card, and management is limited to a particular station, making it non-portable, as opposed to the present '899 Application's claims "combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm, to authorize or deny said user activity", which allows fully portable access and management.

3) U. S. Patent No. 4,956,769, Smith

That I have reviewed U. S. Patent No. 4,956,769, Smith, and find that it relates to a security system for a fixed installation, "in a computer system" (Column 1, line 58), and "capable of limiting the access of some selected users and terminal locations to *** operations on selected database records and fields." (Column 1, lines 9-12).

a) Smith provides access tables or rules (column 3, line 67 - column 4, line 1), but those tables do NOT RELATE to user authentication. Rather, any user authentication is a normal host system based logon process, using "at least one system user, identified by a 'userid' or unique user identification symbol, that is accessing the system from at least one terminal location with a terminal address," (Column 1, lines 58-62) (Emphasis added).

Smith constructs a user access profile table and controls access "by parsing the system sign-on by the system user and extracting therefrom the unique user identification symbol." (Column 5, lines 11-59). The parsing is subsequent to the host system logon process and is not itself authentication.

Smith is thus unlike the present '899 Application's claimed, e.g. Claim 1, "user table comprising at least a unique user identifier for each authorized user and at least one permitted activity said user is authorized to conduct with respect to said data storage media, said user identifier, when combined with a user authentication message from said authorized user in accordance with a predetermined algorithm, authorizes said user".

Thus, Smith does not add a portable security system to Anderl et al. related to the user table based authentication of the present '899 Application.

b) Further, Smith does not add portability of a security system to Anderl et al.

Rather, Smith discusses "Specifically, the user access profile table and the terminal location security access table are constructed within the host system environment ***." (Column 5, lines 9-12).

Thus, Smith access is established at installation time, and is conducted within the host system, making it non-portable, as opposed to the claims of the present '899 Application which specify "combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm, to authorize or deny said user activity", which allows fully portable access and management.

4) Anderl et al. and Smith:

The combination of Anderl et al. and Smith teaches against the present '899 Application's "portable security system comprising *** a computer processor mounted in said portable data storage cartridge ***; *** having a user table comprising at least a unique user identifier for each authorized user ***; said computer processor *** combining said user authentication message with at least part of said user identifier from said user table in accordance with said predetermined algorithm to authorize or deny said user activity ***."

Instead, the authorization of Smith is a normal sign-on within the host system, and is non-portable, and the Anderl et al. access security is provided by an entirely different mechanism, and is established at issuance of the card at a particular station, all as discussed above. Thus, both Smith and Anderl et al. teach against the portable authentication of the '899 Application.

That the undersigned declares further that all statements made herein of his own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patents issuing thereon.

Further declarant saith not.

Date: July 12, 2005 /s/

Paul M. Greco